AMENDMENT TO THE CLAIMS

Please **AMEND** claims 1, 3, 9, 13-15, 21, and 22 as follows.
Please **CANCEL** claims 2, 11, 12, and 20 as follows.
Please **ADD** claims 23-25 as follows.

A copy of all pending claims and a status of the claims are provided below.

1. (Currently Amended) A method for authentication in a network, the method comprising:

creating a credential string on a portal server, the credential string being an encrypted hash of ~~which is derived from~~ a session ID;

sending a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;

receiving a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including ~~which includes~~ the credential string; and

sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

2. (Canceled)

3. (Currently Amended) The method of claim 1 ~~2~~, wherein the ~~credential string is an~~ encrypted hash of the session ID is a derivate of the session ID.

4. (Original) The method of claim 1, further comprising the steps of:

performing a lightweight directory access protocol (LDAP) lookup using the UserID; and

if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application.

5. (Original) The method of claim 1, wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory.

6. (Previously Presented) The method of claim 1, further comprising the steps of:

sending the UserID associated with the session ID and the credential string to a software application proxy;

checking whether the session ID and the credential string have been previously received within a predetermined time period; and

if affirmative, initiating a security breach procedure.

7. (Original) The method of claim 6, wherein the security breach procedure causes the termination of any session associated with the UserID.

8. (Original) The method of claim 1, wherein the receiving step and sending a response step is performed by an authentication proxy.

9. (Currently Amended) A method for authenticating a user request for a software application, the method comprising:

receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of ~~is derived from~~ a session ID, which is created at a portal;

sending a confirmation request from the authentication proxy to the a portal while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal, the confirmation request includes the credential string;

receiving a response at the authentication proxy for the confirmation request while maintaining the user password on the portal such that the user password is not required to authenticate the User ID; and

validating the UserID using a light weight directory access protocol (LDAP) lookup request and the response.

10. (Original) The method of claim 9, further comprising providing a confirmation to the software application if the response is affirmative and the UserID is authenticated by the LDAP lookup.

11. (Canceled)

12. (Canceled)

13. (Currently Amended) The method of claim 10 ~~12~~, further comprising validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy.

14. (Currently Amended) The method of claim 9, further comprising receiving the UserID and a the user password during a logon to the portal, wherein the UserID is validated in the validating step and the user password is maintained at the portal and used to process the confirmation request.

15. (Currently Amended) A system for authenticating a session stored on a computer readable storage medium, comprising computer readable program code, comprising:

an authentication proxy which receives requests to authenticate a UserID and a credential string, the credential string being an encrypted hash of a session ID and created on a portal; and

a credential string validation component which receives requests to validate the credential string while maintaining a user password on the portal such that the user password is not required to validate the credential string,

wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

16. (Original) The system of claim 15, wherein the authentication proxy performs lightweight directory access protocol (LDAP) lookups using the UserID and sends the credential string to the credential string validation component and receives a validation reply.

17. (Original) The system of claim 16, wherein the authentication proxy sends an affirmative authentication reply to a software application when both the LDAP lookup is successful and the validation reply indicates a valid credential string.

18. (Original) The system of claim 17, wherein the authentication proxy receives the UserID and credential string from a software application.

19. (Previously Presented) The system of claim 15, further comprising a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string have been previously received within a predetermined time period.

20. (Canceled)

21. (Currently Amended) The system of claim 15, further comprising:

~~a portal for accepting a logon by a user and for creating the credential string from an associated session ID;~~

a lightweight directory access protocol (LDAP) directory for authenticating the UserIDs and which is accessible by the authentication proxy; and

a software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string.

22. (Currently Amended) A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product including at least one program code to:

create a credential string on a portal server, the credential string being an encrypted hash of ~~which is derived from~~ a session ID;

send a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;

receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including ~~which includes~~ the credential string; and

send a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

23. (New) The system of claim 15, wherein the UserID and the credential string are sent to a software application when the predetermined time period has elapsed.

24. (New) The system of claim 23, wherein a network security breach is initiated when a second request to validate the credential string occurs within the predetermined time period of a first request to validate the credential string.

25. (New) The system of claim 24, wherein the portal is configured to accept a logon by a user and create the credential string from an associated session ID.